L4: Entry 32 of 64 File: USPT

DOCUMENT-IDENTIFIER: US 6381631 B1
TITLE: Method and apparatus for controlling client computer systems

Brief Summary Text (5):
One way of determining which files should be installed on the client computer system is to have the client management software provide the server management software with some form of identification of the user of the client computer system. For example, the client management software can supply to the server management software a name or a type of a user of the client computer system. The server management software uses the name or type of the user to determine which files that user or type of user should have and then sends the appropriate files or instructions or both to the client management software.

Brief Summary Text (6):
For example, all supervisors of a company may receive updated salary information every Monday morning. The client management software in a particular client computer system used by a supervisor can be preprogrammed with the supervisor's name or title and the client management software can provide this information to the server management software. The server management software can provide updated salary information to the client management software based on the information it receives from the client management software. In contrast, client management software on a different computer identifying the user as an employee would not receive this updated salary information because the server management software will only send this information to supervisors.

Detailed Description Text (22):
When the connection is established, log in manager 232 passes the certificate that was sent to the remote network, similar information, or information corresponding to the certificate or similar information to client manager 240. This may include the name of the user and a public key of the user. Client manager 240 sends some or all of this information to the server management software of the remote system for authentication. Client manager 240 may receive a certificate or other authentication information from the server management software, which may be used to authenticate the server management software as described above.

Detailed Description Text (31):
In one embodiment, while server management software and client manager 240 are communicating as described above, server management software can send information about other networks with which the client is allowed to communicate to client manager 240. Such other networks may be third party networks or other remote networks. This allows a system administrator to determine the remote networks a user is allowed access in addition to determining third party networks the user is allowed to access. Client manager 240 stores this information in an "other network file" in trusted network storage 242, which may be memory or disk. The information may be a list of names and contact instructions (e.g. dialing sequences and commands sequences used to log in) used to contact the other network. In one embodiment, connection manager 220 allows the user to contact only those networks identified in trusted network storage 242, including the remote network as described below. This way, connection manager 220 enforces the requirement that any other network contacted by the user is listed as trusted.

Detailed Description Text (43):
The user is prompted 310 for identification information and the identification information is received 310 as described above. The identification information may be locally authenticated 312 as described above. If the identification is locally authenticated, and the authentication fails 314, the user may be warned 316 that he will have to identify himself again and an optional counter may be incremented 316,

having been initialized to zero in a step not shown that precedes step 310, and the method continues at step 310. If the counter reaches a threshold value, the system may be locked 316 as described above.

WEST

Generate Collection Print

L4: Entry 45 of 64 File: USPT

DOCUMENT-IDENTIFIER: US 6098099 A
TITLE: Third-party notification by network directory server

Brief Summary Text (15):
When the IP payload is encrypted end-to-end using a protocol such as IP-sec, an intermediate box is unable to obtain information such as port numbers necessary to mark data. However, the intermediate box is responsible for ensuring that an untrustworthy user workstation, e.g., a directory client, is not sending improperly marked data across the network.

Brief Summary Text (23):
Such an arrangement provides a monitoring mechanism for tracking network access requests, particularly those originating from untrustworthy users, such as hackers, who attempt to alter the priority levels of message requests through the network. In such instances, the directory server can notify a third-party in charge of an occurrence of a particular network access request and other related information (e.g., origin, results, etc.). The third party need not have an existing connection with the directory server. This allows the third party to take preventive measures to maintain the priorities associated with network access requests, particularly those defined by service level agreements. Such preventive measures may include transmitting a warning message to the individual or device that is responsible for the network access request, preventing the responsible individual/device from accessing the network or any other suitable measures that will deter individuals from tampering with the priorities of message requests for the network. As such, the present invention eliminates the problems associated with update lag, server overload and encrypted data.

Detailed Description Text (2):
FIG. 1 illustrates a system overview of a network 10 employing a centrally administered directory server for managing the service quality of the network environment, in accordance with the present invention. Network 10 includes a network backbone 101 connected between a plurality of network nodes. Network 10 also includes several other nodes 105, 107, 109 which act as clients (hereinafter "client(s)") of a directory server 103, such as a workstation. Client(s) 105, 107, 109 interact with directory server 103, across communication links and nodes of network 10, to regulate service quality and data transmission, across network backbone 101. Directory server 103 also notifies a designated third-party or parties, generally indicated by the reference numeral 111, upon an occurrence of a specified event, such as if directory information of directory server 103 is accessed and/or modified, specifically by an untrustworthy client of directory server 103. The incorporation of such a third-party notification feature allows third party 111 to enforce traffic class priorities and access characteristics and to ensure that an untrustworthy client is not sending improperly marked data, across network backbone 111.

Detailed Description Text (3):
That is, such an arrangement provides a monitoring mechanism for tracking network access requests, particularly those originating from untrustworthy users, such as hackers, who attempt to alter the priority levels of message requests through the network. In such instances, the directory server can notify a third-party in-charge of an occurrence of a particular network access request and other related information (e.g., origin, results, etc.). This allows the third party to take preventive measures to maintain the priority levels of message requests through the network, particularly those priority levels defined by service level agreements. Such preventive measures may include transmitting a warning message to individual/device (e.g., the sender) that is responsible for the network access request, preventing the responsible individual/device from accessing the network or any other suitable measures that will deter individuals from tampering with the priorities of message requests through the

network.

WEST

Generate Collection Print

L4: Entry 49 of 64 File: USPT

DOCUMENT-IDENTIFIER: US 6038399 A
TITLE: Computer manufacturing architecture with two data-loading processes

Detailed Description Text (52):
FIG. 1 shows an architectural overview in block diagram form of the hardware, interconnectivity, and data distribution flow preferably used to embody the novel computer manufacturing software installation system. This system is designed to provide efficient software distribution, configuration, installation, and tracking of software and hardware. The software distribution and installation system allows for release of software by one or more software engineering groups 102, each with its own development schedule, into a database network 104 which eliminates any duplicate files which may exist between groups and between versions of software released by the same group. The resulting database and software files are distributed to various master database servers 106 at remote manufacturing facilities. From these master databases, software is distributed to one or more local databases and their associated servers 108 for download onto personal computers in either a predetermined ("as configured"), build-to-order, or configure-to-order configuration. In parallel with the above described distribution of software files, rules for the configuration of the software are created and distributed, again by one or more software engineering groups 102, through the configuration and tracking system. The product configurations are released into a separate database network 110. The resulting information is distributed to various CCP servers residing at remote manufacturing facilities 112. Once both the software and configuration rules have been distributed to the manufacturing facility, software pre-installation can commence. The process communicates with the product configurations database 112. The product configurations database 112 holds information concerning configurations for particular assembled units and hard drives as well as the rules for configuring new units and hard drives. A process is run at the manufacturing facility on a client station 114 which accesses the product configuration database 112 and allows a hardware and software configuration list to be created or changed if it already exists. This process also references and enforces the rules of hardware and software configuration contained on the database 112. Once a configuration list has been created, the assembled unit (or raw hard drive in a surrogate machine) 116 is connected to the network. A separate process running on the assembled unit 116 accesses the product configuration database 112 and retrieves its configuration list. The process then accesses a local software database 108 and commences the actual download of information onto its hard drive. Once the software has been downloaded successfully, diagnostic checks are performed and software set-up routines are run on the assembled unit 116 and product configuration database 112 is updated to reflect that a software pre-installation has taken place for the particular machine 116. The configuration list for the particular machine can then be used as "as built" data. This data is transmitted back to a database network 118 at manufacturing headquarters. This "as built" information can then be distributed to customer service systems 120 including service centers 122 which can rebuild a customer's hard drive based on the "as built" information. The information can also be used by royalty tracking systems 124 to ensure appropriate payment to third-party software providers and configuration and failure analysis systems 126 to evaluate diagnostic, download completion, and other data related to software pre-installation.

Detailed Description Text (62):
The first method 302 is via the Consolidated Image Importer Tool (CIIT), a utility that can be used by a software engineering group to "check" software into the group's database 106. CIIT is run on a machine known as a "golden master" which contains "installed" versions of the software to be released to the software distribution system by the software engineering group. CIIT will import every file from the "golden master", including the boot sector, partition, and all directory information, into the engineering entity's database. Any duplicate files are eliminated during the import

process. To organize the production files for database entry, the software versions are grouped together as a Stock Keeping Unit (SKU)/Bill of Materials (BOM) combination. The SKU identifies the CPU, the primary hard disk, the country/keyboard, and whether software will be pre-installed in the factory during manufacture. A BOM is a list of the software files which will be copied to a computer during factory software pre-installation. A BOM is the identifier used to recall a specific disk image and is used by a software engineering group for tracking the image. The disk image referenced by the BOM represents what the engineering entity wants the customer to see when he or she boots their computer for the first time. Both the SKU and BOM are used by the software download database and the software download process (GEMINI) to ensure that all necessary software will be downloaded at the computer manufacturing facility's software pre-install.

WEST

Generate Collection Print

L4: Entry 45 of 64 File: USPT

DOCUMENT-IDENTIFIER: US 6098099 A
TITLE: Third-party notification by network directory server

Brief Summary Text (15):
When the IP payload is encrypted end-to-end using a protocol such as IP-sec, an intermediate box is unable to obtain information such as port numbers necessary to mark data. However, the intermediate box is responsible for ensuring that an untrustworthy user workstation, e.g., a directory client, is not sending improperly marked data across the network.

Brief Summary Text (23):
Such an arrangement provides a monitoring mechanism for tracking network access requests, particularly those originating from untrustworthy users, such as hackers, who attempt to alter the priority levels of message requests through the network. In such instances, the directory server can notify a third-party in charge of an occurrence of a particular network access request and other related information (e.g., origin, results, etc.). The third party need not have an existing connection with the directory server. This allows the third party to take preventive measures to maintain the priorities associated with network access requests, particularly those defined by service level agreements. Such preventive measures may include transmitting a warning message to the individual or device that is responsible for the network access request, preventing the responsible individual/device from accessing the network or any other suitable measures that will deter individuals from tampering with the priorities of message requests for the network. As such, the present invention eliminates the problems associated with update lag, server overload and encrypted data.

Detailed Description Text (2):
FIG. 1 illustrates a system overview of a network 10 employing a centrally administered directory server for managing the service quality of the network environment, in accordance with the present invention. Network 10 includes a network backbone 101 connected between a plurality of network nodes. Network 10 also includes several other nodes 105, 107, 109 which act as clients (hereinafter "client(s)") of a directory server 103, such as a workstation. Client(s) 105, 107, 109 interact with directory server 103, across communication links and nodes of network 10, to regulate service quality and data transmission, across network backbone 101. Directory server 103 also notifies a designated third-party or parties, generally indicated by the reference numeral 111, upon an occurrence of a specified event, such as if directory information of directory server 103 is accessed and/or modified, specifically by an untrustworthy client of directory server 103. The incorporation of such a third-party notification feature allows third party 111 to enforce traffic class priorities and access characteristics and to ensure that an untrustworthy client is not sending improperly marked data, across network backbone 111.

Detailed Description Text (3):
That is, such an arrangement provides a monitoring mechanism for tracking network access requests, particularly those originating from untrustworthy users, such as hackers, who attempt to alter the priority levels of message requests through the network. In such instances, the directory server can notify a third-party in-charge of an occurrence of a particular network access request and other related information (e.g., origin, results, etc.). This allows the third party to take preventive measures to maintain the priority levels of message requests through the network, particularly those priority levels defined by service level agreements. Such preventive measures may include transmitting a warning message to individual/device (e.g., the sender) that is responsible for the network access request, preventing the responsible individual/device from accessing the network or any other suitable measures that will deter individuals from tampering with the priorities of message requests through the

network.

WEST

Help | Logout | Interrupt

Main Menu | Search Form | Posting Counts | Show S Numbers | Edit S Numbers | Preferences | Cases

Search Results -

Terms	Documents
L4 and (healthcare or hospital or service adj provid$3 or pharmac$3 or drug)	32

Database: US Patents Full-Text Database; US Pre-Grant Publication Full-Text Database; JPO Abstracts Database; EPO Abstracts Database; Derwent World Patents Index; IBM Technical Disclosure Bulletins

Search: Refine Search

Recall Text | Clear

Search History

DATE: Tuesday, July 30, 2002 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
DB=USPT,PGPB,JPAB,EPAB,DWPI,TDBD; PLUR=YES; OP=ADJ			
L5	L4 and (healthcare or hospital or service adj provid$3 or pharmac$3 or drug)	32	L5
L4	L3 and (broadcast$3 or transfer$4 or transmit$4 or send$3) near5 (document or file or information or data) same (consumer or customer or client)	64	L4
L3	L2 and (warn$3 or recall$3 or safety advisory)	64	L3
L2	(broadcast$3 or transfer$4 or transmit$4 or send$3) near5 (document or file or information or data) same (consumer or customer or client) same third party	397	L2
DB=USPT; PLUR=YES; OP=ADJ			
L1	6119164.pn.	1	L1

END OF SEARCH HISTORY

WEST

Help | Logout | Interrupt

Main Menu | Search Form | Posting Counts | Show S Numbers | Edit S Numbers | Preferences | Cases

Search Results -

Terms	Documents
L10 and (broadcast$3 or transfer$4 or transmit$4 or send$3) near5 (document or file or information or data) same (consumer or customer or client)	9

Database: US Patents Full-Text Database
US Pre-Grant Publication Full-Text Database
JPO Abstracts Database
EPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search: L12

Refine Search

Recall Text | Clear

Search History

DATE: Tuesday, July 30, 2002 Printable Copy Create Case